FULL STACK ACADEMY

www.fullstackacademy.in 9015 236 236

SOC ANALYST

1. **Introduction to SOC**
2. **Fundamentals of networkings**
3. **SIEM technology**
4. **Phishing with details analysis**
5. **Endpoint Security**
6. **Threat Hunting with tools**
7. **End Point security**
8. **XDR VS EDR**
9. **Malwares and categories of malware**

INTRODUCTION TO SOC

Introduction to SOC Analyst: Roles and Responsibilities
Functions of SOC, MITRE Attacks Framework, Lockheed Cyber Kill Chain
Bianco: Pyramid of Pain, Unified Cyber Kill Chain

FUNDAMENTALS OF NETWORKINGS

Fundamentals of Cybersecurity Frameworks, Information Security Policy
OSI Model, TCP/IP, Windows Fundamentals, Network Protocols, Emphasises on End-to-End SOC Workflow

SIEM TECHNOLOGY

Security Information and Event Management, Introduction to Incident Response and Handling, Introduction to SIEM, Splunk Setup and Basics, Incident Detection, Investigation, and Response with Splunk, Learn Incident Detection withSIEM

PHISHING WITH DETAILS ANALYSIS

Introduction to Phishing, Phishing Fundamentals
Real-World Phishing Campaign, Analysis of Phishing
Windows logs analysis

ENDPOINT SECURITY

Introduction to Endpoint Security, Windows Internals Windows Event Logs, Sysinternals, Antivirus, ePO

THREAT HUNTING WITH TOOLS

Threat Hunting with Alien Vault, Introduction to Threat Hunting
Incident Response vs Threat Hunting, Alien EDR
MITRE Adversary Simulation Enhance Incident Detection with Threat Intelligence

END POINT SECURITY

What is Trellix EDR, Trellix EDR Setup
MITRE Adversary Simulation, Atomic Red Team,
IOC Threat Hunting with Trellix EDR

XDR VS EDR

Introduction to XDR
EDR vs XDR

MALWARES AND CATEGORIES OF MALWARE

IIntroduction to Malware, Malware Analysis
Types of Malwares, Case Study
Sandboxing, Hands on learning